WHITE PAPER

GILLIAM SECURITY

Third Party Security Risk Management

Understanding security risks of using a third party.

From acquisitions to mergers to software having integrations with systems outside of your organization's span of control, third party security risk management has never been more important.

One of the most famous examples where third party risk management failed was the acquisition of the Starwood brand by Marriott in 2016.

Impact of Third Party Risk Management

In 2016, Marriott acquired the Starwood brand to include internal guest reservation database. This system had several million records. In a press release dated January 4, 2019 by Marriott (link), this data included passport numbers and payment card numbers.

Why is this a failure of risk management? There are a couple of item that are of critical importance:

- The Federal Trade Commission reported the breach started as early as 2014, which was prior to the acquisition of the Starwood brand by Marriott; and,
- Regardless of fault, the Marriott name was referenced in the breach which makes a difference of brand equity.

As a consequence of this breach, Marriott has since spent a substantial amount of money in legal fees. In addition to legal fees, regulatory fines took place. An example of one fee is from the UK Information Commissioner's Office ("ICO") where Marriott was fined £18.4million. You may read more detail on this here.

Benefit to Third Party Risk Management

One of the benefits to third party risk management is discovering potential issues before an organization "assumes the risk." *Below is an example and has had all names, dates and statements of facts redacted to protect the anonymity of the client.*

In 2018, a widget company called ACME Brick ("ACME") decided to engage in business with WIDGET Express ("WIDGET"). As part of the ACME's onboarding prior to contract signature with WIDGET, the third party security risk management team performed a series of security assessment on WIDGET to include:

An application security assessment of each application within the scope and network boundary where ACMEs data was to be hosted;

- A vulnerability assessment of each application within the scope and network boundary where ACMEs data was to be hosted;
- A vulnerability assessment of ingress and egress points where ACMEs data was to be hosted;
- A logical penetration test of applications where ACMEs data is hosted; and,
- A physical security assessment of the facilities where WIDGET processed ACMEs data.

As part of the performance of these tests, several security risks were identified. In some cases, the risks exceeded the risk appetite of ACME.

Effective Third Party Risk Management

In order for third party risk management to be effective, an organization needs to define an approach as well as a risk appetite and threshold.

It is pivotal to have each item because:

- A defined approach will enable a baseline and consistency to measure against. Not having a baseline will result in inconsistent results, thereby making the results subjective to human interpretation. This usually results in an ineffective program.
- A risk appetite and threshold are important because an organization needs to have defined parameters to understand when a vendor is exceeding predefined criteria. This will also help the business owner within the organization understand if they are willing to accept the risk with the potential of making substantially more revenue than the risk would cost.

Using a Third Party for Third Party Risk Management

A third party can be used for third party risk management as long as the details you receive for the details of the tertiary parties evaluated align to the assessment requirements that would be performed by your organization if the third party risk management function was performed by internal resources.

Need help establishing this function or would like to outsource this function? Reach out to Gilliam Security today and we would be glad to help answer questions and help you out.

Why Gilliam Security?

Gilliam Security has recognized consultants from major fortune 500 companies with certifications such as the CISSP, CISM, CISA and CRSIC. Each consultant also has experience in building the information security, as well as privacy, function from inception to maintaining operations.

Contact Us Today at sales@gilliamsecurity.com